	See '203 claim 9		See '203 claim 10
NetStalker (publicuse/on sale)	See '203 claim 9		See '203 claim 10
Ç <b>isim</b> Lerin	plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.  The system of claim 12, wherein the plurality of network	monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network	The system of claim 20, wherein an enterprise monitor associated with a
#203 #203 *Claim*	50		21

NetStalker and HP OpenView

HP OpenView sale).						
203 NetStalker Claim Term (public use/on salummer)	plurality of domain	monitors is adapted	to automatically	receive and integrate	the reports of	suspicious activity.

TH OpenView (printed publication and public use)	See '203 claim I	See '203 claim 1	See '203 claim 1	See '203 claim 1
NetStalker (public use /.on sale)	See '203 claim 1	See -203 claim 1	See '203 claim 1	See '203 claim I
Claim Term	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	plurality of nitors in the twork;	fwork s network	n analysis of network are selected from one of the following es: {network packet rester or namends, retwork packet data transfer network packet data inetwork packet data inetwork connection b, network connection c, network connection rk packet, network in acknowledgements, work packets indicative known network-service
Cash number	-			

330601\_2

HP Open View (printed publication and public use)	See '203 claim 1	See '203 claim 1	Sec '203 claim 2		See '203 claim 3	See '203 claim 4	See '203 claim 5
NetStalker (public use / on sale)	See '203 claim 1	See '203 claim 1	Sec · 203 claim 2		See '203 claim 3	See '203 claim 4	See '203 claim 5
Claim Term.	protocols); generating, by the monitors, reports of said suspicious	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	The method of claim 1,	wherein megrating comprises correlating intrusion reports reflecting underlying commonalities.	The method of claim 1, wherein integrating further comprises invoking counterneasures to a suspected attack	The method of claim 1, wherein the plurality of wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	The method of claim 1, wherein the enterprise network
r615 Celam number			7		6	4	5

HP OpenView (printed public use)	"To start a discovery, you need to know some information about your own network and the networks you want Autodiscovery to search. To run an IP discovery, you must provide the following information:  The IP address and community name for your default gateway or router if present." (2-2) [SYM_P_0080966]	"Devices in the network are displayed on maps. Devices and subnetworks can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network function, network organization, or corporate organization. You can use the maps to manage your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background. Changes in network status are displayed on network maps with icons representing devices. Color is used to indicate device status. Submaps allow you to create several views of your network to simplify management. You can add meaningful graphics such as geographic maps and floor plans as backgrounds for your map to provide "real world" visual references for your network." (1-2) [SYM_P_0080958]
*	"NetStalker monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, NetStalker automatically identifies network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real using information stored in an internal database, the misuse signature database." p. 1-2. [SYM_P_0079560]	
*615 Cham number	Is a ICP/IP network.  The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	

4			· · · · · · · · · · · · · · · · · · ·	, s
(Sur	twork rs. symbol		llection of nats.  Int. Int. Int. Idements. Idements. Incent anagement attations. If P) is use in the	example m, it is register rder to
nublic	rious ne ultiplexe or delete 0080996		angement and angement and angement and angement and angement and angement and angement a generit a between the between ants in the angement and	may, for n additio will also ree, in o echanism
rView rand	s, and m symbols SYM P	쉳	rral mod d d newood d d newood cecute m control n cich as ho iich have g the net or mana nt Protoo ormation d the age	nterprise ubtree. I nterprise this subf
HP OpenView	ool set co os, router can add (3-14) [	жи геро	rrchitecturations and attions and attions are tations and attions and a tion and a like, where the network and attions and attinuous and attin	ee, the er in this si hat the e ns under s identifi
HP OpenView (printed publication and public use)	"The Component symbol set contains various network components such as hubs, routers, and multiplexers. OpenView applications can add symbols or delete symbols from the standard set." (3-14) [SYM_P_0080996]	See Figure 12 in my expert report.	"Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements." (RFC 1157 p. 4) [SYM_P 0527111]	"Upon receiving a subtree, the enterprise may, for example, define new MIB objects in this subtree. In addition, it is strongly recommended that the enterprise will also register its networking subsystems under this subtree, in order to provide an unambiguous identification mechanism for use in
printe	Compon nents su /iew app he standa	gure 12 i	cti in the rk managark managark managark ations what element at server responsi ons reque implie Ne implie Ne immicat k managark	new MII Iy recom working
	"The compo	See Fi	-Impli netwo Netwo Applica Netwo termin agents functif The Si to corn netwo	"Upon define strong its net
sale)	And the second s			
NetStalker offc.use/on				
NetStalker (public use/ on sale)				
<b>.</b>				
and the second				
Qaim				
i Y				
'615 Claim nimber				

HP OpenView (printed publication and publicase)	management protocols. For example, if the "Flintstones, Inc." enterprise produced networking subsystems, then they could request a node under the enterprises subtree from the Internet Assigned Numbers Authority. Such a node might be numbered:	1.3.6.1.4.1.42	The "Flintstones, Inc " enterprise might then register their "Fred Router" under the name of:	1.3.6.1.4.1.42.1.1" (RFC 1155 p. 6) [SYM_P_0501017]	"See also the Host and Gateway Requirements RFCs for more specific information on the applicability of this standard." (RFC 1155 p. 1) [SYM_P_0501013]	"sysServices OBJECT-TYPE	layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., IP gateways) 4 end-to-end (e.g., IP hosts) 7 applications (e.g., mail relays)
NetStalker (publicuse / on sale)							
Claim Term							
·615. Claim							

46

330601\_2

(printed publication and public use)	and 6 may also be counted." (RFC 1213 p. 14)  [SYM_P_0501155-SYM_P_0501156]	"ipForwarding OBJECT-TYPE SYNTAX INTEGER {   forwarding(1) acting as a gateway   not-forwarding(2) NOT acting as a gateway }, (RFC 1213 p. 25) [SYM_P_0501165]	"Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these remote probes are stand-alone devices An organization may employ many of these devices, one per network segment, to manage its internet." (RFC 1271 p. 3) [SYM_P_0501208]	103:	See Feather, Frank Edward, Ph.D., "Fault Detection in an Ethernet network via anomaly detectors", Carnegie Mellon University, Order number 9224199, 1992 [SYM_P_0501779- SYM_P_0502036].	See '203 claim 8
NetStalker (public use/ on sale)						See '203 claim 7
Koise Claim Claim Term number				The method of claim 1,	wherein at least one of salar network monitors utilizes a statistical detection method.	The method of claim 1,

330601\_2

#### HP OpenView See '203 claim 10 See '203 claim 8 See '203 claim 9 See '203 claim 10 See '203 claim 9 See '203 claim 8 domain monitor with respect to among multiple domains of the wherein deploying the network wherein deploying the network enterprise monitor with respect monitors includes deploying a a plurality of service monitors integrating is performed by an plurality of domain monitors within the enterprise network, integrating is performed by a plurality of service monitors within the domain monitor's corresponding domain of the monitors includes placing a each domain monitor being associated network domain. The method of claim 10, The method of claim 1, The method of claim 8, to a plurality of domain wherein receiving and wherein receiving and enterprise network. enterprise network. associated with a 9 Ξ

330601\_2

terprise See '615 claim 1	1615 Chime	Claim Term	NetStalker fourblicture / on sale)	HP OpenView (printed publication and publication)
monitors within the enterprise network.  An enterprise network monitors See '615 claim 1 monitoring system comprising: a plurality of network monitors See '615 claim 1 metwork. safe plurality of network monitors detecting suspicious network activity based on analysis of network packet from one or more of the following categories: fnetwork packet data transfer commands, network packet data transfer errors, network packet data transfer errors, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packet, network connection acknowledgements, said network packets indicative of well-known network-service protocols!; said network monitors See '615 claim 1  See '615 claim 1  Traffic data selected from one or more of the following categories: fnetwork packet data volume, network packet data volume, network packet, network connection acknowledgements, and network packets indicative of well-known network-service	number	100 April 1		
An enterprise network  An enterprise network monitors  a plurality of network monitors  deployed within an enterprise  network.  said plurality of network  monitors detecting suspicious  network activity  based on analysis of network  traffic data selected from one or more of the following  categories: {network packet  data transfer commands,  network packet data  volume, network connection  requests, network connection  requests, network connection  denials, error codes included in  a network packet, network  connection acknowledgements,  and network packets indicative  of well-known network-service  protocols};  See '615 claim 1		monitors within the enterprise		
monitoring system comprising:  a plurality of network monitors deployed within an enterprise network.  said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols}; said network monitors See '615 claim 1	**	iictwoin.	San 66 15 about	Coo 615 claim 1
See '615 claim 1 See '615 claim 1 See '615 claim 1 See '615 claim 1	3	An enterprise network	Sec '013 ciaim i	Sec 015 claim I
See '615 claim 1 See '615 claim 1 See '615 claim 1	•	monitoring system comprising:		
See '615 claim 1 See '615 claim 1	···	a plurality of network monitors	See '615 claim 1	See '615 claim 1
See '615 claim 1 See '615 claim 1		deployed within an enterprise		
See '615 claim 1 See '615 claim 1 See '615 claim 1		network,		
See '615 claim 1		said plurality of network	See '615 claim 1	See '615 claim I
See '615 claim 1		monitors detecting suspicious		
See '615 claim 1		network activity		W/ 10 (V/
See '615 claim 1		based on analysis of network	See '615 claim I	See '615 claim 1
See '615 claim 1		traffic data selected from one		
See '615 claim 1		or more of the following		
See '615 claim 1	•	categories: {network packet		
See '615 claim 1		data transfer commands,		
See '615 claim 1		network packet data transfer		
See '615 claim 1		errors, network packet data		
See '615 claim 1		volume, network connection		
See '615 claim 1		requests, network connection		
See '615 claim 1		denials, error codes included in		
See '615 claim 1		a network packet, network		
See '615 claim 1		connection acknowledgements,		
See '615 claim 1		and network packets indicative		
k monitors See '615 claim 1		of well-known network-service		
See '615 claim 1		protocols};		
		said network monitors	See '615 claim 1	See '615 claim 1

'615. 'Claim number	Glaim Term	NetStalker (public use / onsale)	HP OpenView (printed publication and public use)
	generating reports of said		
	one or more hierarchical	See '615 claim 1	See '615 claim 1
	monitors in the enterprise		
<b>M</b>	network, the hierarchical		
	monitors adapted to		
	automatically receive and		
	integrate the reports of		
	suspicious activity.		
14	The system of claim 13,	See '203 claim 2	See '203 claim 2
	wherein the integration		
	comprises correlating intrusion		
	reports reflecting underlying		
	commonalities.		
15	The system of claim 13,	See '203 claim 3	See '203 claim 3
	wherein the integration further		
,	comprises invoking		
	countermeasures to a suspected		
	attack.		
91	The system of claim 13,	See '203 claim 4	See '203 claim 4
	wherein the plurality of		
*********	network monitors include an		
	application programming		
	interface (API) for		
	encapsulation of monitor		
	functions and integration of		

Toguna Toguna	Claim Term	(public use // on sale)	(printed publication and public use) 😤
#	third-party tools.		
T T	The system of claim 13,	See '203 claim 5	See '203 claim 5
3 .2	wherein the enterprise network is a TCP/IP network.		
TT 81	The system of claim 13,	See '615 claim 6	See '615 claim 6
3	wherein the network monitors		
<u>a</u>	are deployed at one or more of		
4	the following facilities of the		
<u></u>	enterprise network: {gateways,		
ou L	routers, proxy servers}.		
H 61	The system of claim 13,	See '203 claim 7	See '203 claim 7
3	wherein the plurality of		
2	network monitors includes a		
<u>a</u>	plurality of service monitors		
a	among multiple domains of the		
	enterprise network.		C . 1 COC. 1
70	The system of claim 19,	See '203 claim 8	See '203 claim 8
	wherein a dornain monitor		
4	associated with the plurality of		
*	service monitors within the		
<u>*</u>	domain monitor's associated		
	network domain is adapted to		
8	automatically receive and		
·B	integrate the reports of		
S	suspicious activity.		
21 II	The system of claim 13,	See '203 claim 9	See '203 claim 9

.HP OpenView (printed publication and public use)		See '203 claim 10		See '615 claim 1	uters and "To start a discovery, you need to know some information logy, about your own network and the networks you want apts to Autodiscovery to search. To run an IP discovery, you must provide the following information:	The IP address and community name for your default
NetStalker (public use / on sale)		See '203 claim 10		See '615 claim 1	"NetStalker monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, NetStalker automatically identifies network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real using information stored in an internal database, the misuse signature database, in 1-2	[SYM_P_0079560]
Claim Term  wherein the plurality of network monitors include a plurality of domain monitors	within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	The system of claim 21, wherein an enterprise monitor associated with a plurality of	domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	method nitoring prising:	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a	gateway;
'615. (Taim mumber		22		*		

. 615 Claim Claim Term	NetStalker (public use // on sale)	HP OpenView (printed publication and public use).
	"Initial PC Fitter Configuration	
		"Devices in the network are displayed on maps. Devices
	<u> </u>	and subnetworks can be organized into submaps to suit your
		needs. You can create separate submaps of devices grouped
	cate between the NSC router and NetStalker. The filters are	by device function, network function, network organization,
	nd downloaded to the router when you run the shell,	or corporate organization. You can use the maps to manage
	mation on installing	your network from a single display even when the network
	NetStalker." p. 1-4. [SYM P_0079562]	includes devices from different manufacturers. Programs
		that manage hubs, routers, servers, and other network
-	"Securing the Connection	devices can run in the background. Changes in network
		status are displayed on network maps with icons
	Since the Netstalker server platform can be located anywhere on the	representing devices. Color is used to indicate device status.
	network, there is the potential of an attacker manipulating the	Submaps allow you to create several views of your network
	connection between the router and the NetStalker server platform.	to simplify management. You can add meaningful graphics
		such as geographic maps and floor plans as backgrounds for
		your map to provide "real world" visual references for your
		network." (1-2) [SYM_P_0080958]
	routers between the NetStaiker platform and the network, and then to	
		"The Component symbol set contains various network
		components such as hubs, routers, and multiplexers.
	ween the NetStalker platform and client is encrypted on the	OpenView applications can add symbols or delete symbols
	egrity, and	from the standard set." (3-14) [SYM_P_0080996]
-	mutual aumentication of the communicating parties.	
		See Figure 12 in my expert report.
	Alternatively, the NetStalker platform can be located on an individual	
	network segment that is directly connected to a dedicated port on the	

HP OpenView (printed publication and publicanse)	"Implicit in the SNMP architectural model is a collection of network management stations and network elements.  Network management stations execute management applications which monitor and control network elements.	Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations.  The Simple Network Management Protocol (SNMP) is used to communicate management information between the	network management stations and the agents in the network elements." (RFC 1157 p. 4) [SYM_P_0527111]	define new MIB objects in this subtree. In addition, it is strongly recommended that the enterprise will also register its networking subsystems under this subtree, in order to provide an unambiguous identification machanism for use in	management protocols. For example, if the "Flintstones, Inc." enterprise produced networking subsystems, then they could request a node under the enterprises subtree from the Internet Assigned Numbers Authority. Such a node might be numbered:	1.3.6.1.4.1.42
NetStalker (publicuse/.on sale)	router it is monitoring." p. 1-4. [SYM_P_0079562]  "Before Netstalker can protect your network, you must configure the	program for your site by setting up the rolliers to be monitored. This chapter describes how to add and edit client routers listed in the NetStalker window. It also describes how to verify the client information " pp. 3-1-3-6. [SYM_P_0079577-SYM_P_0079582]				
Claim Claim Interm						

HP OpenView (printed publication and public use)	The "Flintstones, Inc." enterprise might then register their "Fred Router" under the name of:	1.3.6.1.4.1.42.1.1" (RFC 1155 p. 6) [SYM_P_0501017]	"See also the Host and Gateway Requirements RFCs for more specific information on the applicability of this standard." (RFC 1155 p. 1) [SYM_P_0501013]	"sysServices OBJECT-TYPE	layer functionality  1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., IP gateways) 4 end-to-end (e.g., IP hosts) 7 applications (e.g., mail relays)	For systems including OSI protocols, layers 5 and 6 may also be counted." (RFC 1213 p. 14) [SYM_P_0501155-SYM_P_0501156]	"ipForwarding OBJECT-TYPE SYNTAX INTEGER { forwarding(1), acting as a gateway
NetStalker (public use/on sale)							
Gis Claim Lem Claim							

HP OpenView (printed publication and public use)	not-forwarding(2) NOT acting as a gateway }" (RFC 1213 p. 25) [SYM_P_0501165]	"Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these	may employ any of these devices, one per network	Segment, to manage its internet. (RTC 12/1 p. 3) [SYM P 0501208]	See '615 claim 1			See '615 claim 1		See '615 claim 1			Coo 1903 olaim 3					See '203 claim 3
					See '615 claim I			See '615 claim 1		See '615 claim 1			Sac 1912 claim 1					See '203 claim 3
. Claim Term					detecting, by the network	monitors, suspicious network	network traffic data;	generating, by the monitors,	reports of said suspicious activity; and	automatically receiving and	integrating the reports of	suspicious activity, by one or	The method of claim 34	wherein said integrating	comprises correlating intrusion	reports reflecting underlying	commonalities.	The method of claim 34,
. (615) Claim number													35	)				36

(public-use/on sale)  (printed publication and public use)  Sec '203 claim 4  Sec '203 claim 1  Sec '203 claim 7
See '20 See '203 c

e e le	(publicuse/on sale) See	(printed publication and publicuse).  See '203 claim 8  See '203 claim 9  See '203 claim 10
to a plurality of domain monitors within the enterprise network.		

615 Glaim number	Claim Jorniy	NetStalkër (public use / on sale)	(printed publication and public use)
44	A compa of hierar monitori an enterp	See '615 claim 1	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network	"NetStalker monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, NetStalker automatically identifies network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real using information	"To start a discovery, you need to know some information about your own network and the networks you want Autodiscovery to search. To run an IP discovery, you must provide the following information:
	monitors is deployed at a router;	stored in an internal database, the misuse signature database. p. 1-2. [SYM_P_0079560]  "Initial PC Filter Configuration	The IP address and community name for your default gateway or router if present." (2-2) [SYM_P_0080966]
		NetStalker has a standard set of named PCF filters that are used on NSC routers with router sensors to produce the messages used to communicate between the NSC router and NetStalker. The filters are created and downloaded to the router when you run the shell,	"Devices in the network are displayed on maps. Devices and subnetworks can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network function, network organization, or corporate organization. You can use the maps to manage
		INSTALL.filters. See Chapter 2 for information on installing NetStalker." p. 1-4. [SYM_P_0079562]  "Securing the Connection	your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background. Changes in network
THE PARTY NAMED AND PARTY NAME		Since the Netstalker server platform can be located anywhere on the network, there is the potential of an attacker manipulating the connection between the router and the NetStalker server platform.	status are displayed on network maps with icons representing devices. Color is used to indicate device status. Submaps allow you to create several views of your network to simplify management. You can add meaningful graphics